REMARKS

No claims have been amended. Claims 4, 6, 10, 11, and 18 were previously canceled. Accordingly, claims 1 - 3, 5, 7 - 9, 12 - 17, and 19 - 29 are currently pending in the application and are presented for reconsideration and reexamination in view of the following remarks.

In the Office Action, claims 1 - 3, 5, 7 – 9, 12 – 17, and 19 - 29 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,747,564 to Mimura et al. in view of U.S. Patent Application Publication No. 2001/0001156 to Leppek.

By this Response the Examiner's rejections have been traversed.

Rejection under 35 U.S.C. § 103(a)

The Examiner rejected claims 1 - 3, 5, 7 – 9, 12 – 17, and 19 - 29 as being unpatentable over Mimura et al. in view of Leppek.

Response

Reconsideration and withdrawal of the rejection are respectfully requested.

To establish a *prima facie* case of obviousness, the Examiner must establish: (1) that some suggestion or motivation to modify the references exists; (2) a reasonable expectation of success; and (3) that the prior art references teach or suggest all the claim limitations. Amgen, Inc. v. Chugai Pharm. Co., 18 USPQ2d 1016, 1023 (Fed. Cir. 1991); In re Fine, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988); In re Wilson, 165 USPQ 494, 496 (C.C.P.A. 1970).

It is respectfully submitted that the combination of references fails to teach or suggest all the claim limitations.

The present invention discloses an asset protection system and method that integrates physical asset security with information asset security in a hosted environment, or in certain circumstances in a user's environment. The hosted environment provides security access, generates reports, triggers alerts, and performs analysis based on usage patterns. Usage patterns of repeat system users are learned, such that an anomalous usage results in corrective action, and include physical entry data, logon and logoff times for various equipment, usage periods and file access for various information technology applications, and ingress/egress operation patterns as viewed from a monitoring device. *See* Abstract.

Independent claim 1 recites, *inter alia*:

"...making access decisions in accordance with usage patterns of the user by using the integration of the processor based physical asset protection and processor based information asset protection to grant rights to the information systems..." (*emphasis added*).

Independent claim 12 recites, *inter alia*:

"...the integrator providing integration of the physical protection and information from the information asset protection module for making access decisions in accordance with usage patterns of the user to grant rights to the information systems..." (*emphasis added*).

Independent claim 20 recites, *inter alia*:

"...and using an integration...for making access decisions in accordance with usage patterns of the user to grant rights to the information systems..." (*emphasis added*).

In response to the previous Amendment, the Examiner argues that "a personal access database" is not clearly claimed, disagrees with Applicants' contentions, and responds that the

arguments are not persuasive. Applicants respectfully refer the Examiner to claims 3, 5, and 23 – 25 of the present invention.

The Examiner also argues that Mimura et al. teaches "transmitting a breach of physical asset protection in the centrally-located hosted environment..." Applicants respectfully submit that Mimura et al. merely transmits verification failures or successes to terminal 165, and not in the centrally-located hosted environment, as claimed.

Regarding the present Office Action, Mimura et al. discloses a security guarantee method and system. Mimura et al. provides a security system for a door 130 of a building 105 of which staff that are authorized in advance can enter and leave and a door 140 for a computer room 110. Entry/exit in/out of the computer room 110 and access to the computer system is guarded by a higher level of security than entry/exit in/out of the building 105. An internal door management device 155 controls opening/closing of the internal door 140 of the computer room 110. *See* column 4, lines 20 - 57.

As discussed in the Applicants' previous response, in Mimura et al. there is no processor-based physical asset protection by triggering a user status change upon valid entry/exit through a door of a building, and no information asset protection reflected by the user status change updated to reflect changes in security access requirements, as recited in independent claims 1, 12, and 20 of the present invention. Again, Mimura et al. also does not make access decisions in accordance with usage patterns of the user by using the integration of the processor to grant rights to the information systems as recited in independent claims 1, 12, and 20. Further, Mimura et al. does not transmit a breach of physical asset protection in the centrally-located hosted environment such

that information asset protection is maintained by denying access thereto as recited in independent claims 1, 12, and 20.

The Examiner cites Leppek in an attempt to cure the deficiencies of Mimura et al. regarding "making access decisions in accordance with usage patterns of the user" as recited in independent claims 1, 12, and 20.

Leppek teaches an integrated network security access control system. Whenever a user initiates access to the network, multiple objects begin generating events. These events are applied to an events analyzer, which logically combines the event data into an output value. This output value is mapped through one or more rule sets producing network control prompts, which may cause the event manager 240 to take action that will controllably intervene in the current network activity for a user of interest, in response to one or more relationships associated with such activity being satisfied. Such controlled intervention by the event manager includes the ability to affect or modify this security association and thereby a user's ability to gain access to or continue to be granted access to another resource object in the network. *See* paragraph [0020].

In the present invention, a repeat system user's usage patterns are "learned" to deny access if the present usage is an anomalous usage that results in corrective action.

In contrast, in Leppek, there is no discussion of a repeat system user, in other words, a user that has usage patterns, such that the present usage can be compared with historic usage, and then re-calculating the usage pattern. Only a user--any user that initiates access is discussed. Further, the usage patterns of the particular user in Leppek are not learned; instead events are generated and monitored to establish a security association with the present activity for a user of interest. Thus, the

controlled intervention in Leppek includes the ability to affect or modify a security association (ability to gain access) to another resource object.

Further, there is no integration of physical and information security in Leppek. However, in the present invention, the transmit a breach of physical asset protection in the centrally-located hosted environment operates such that information asset protection is maintained by denying access thereto as recited in independent claims 1, 12, and 20. Instead, the system in Leppek merely utilizes a mechanism for controlling the ability of a user to have access to and communicate with one of more information resources.

Therefore, Leppek fails to cure the deficiencies of Mimura et al.

Accordingly, Applicants respectfully request that the rejection of claims 1, 12, and 20 under 35 U.S.C. § 103(a) be withdrawn.

Moreover, as dependent claims 2, 3, 5, 7 - 9, 13 -17, 19, and 21 - 29, depend from one of claims 1, 12, and 20, Applicants submits these claims are also allowable for at least similar reasons.

CONCLUSION

In light of the foregoing, Applicants submit that the application is now in condition for allowance. If the Examiner believes the application is not in condition for allowance, Applicants respectfully request that the Examiner call the undersigned attorney.

Respectfully submitted,
NATH & ASSOCIATES PLLC

December 21, 2006

NATH & ASSOCIATES PLLC
112 South West Street
Alexandria, VA 22314-2891
Tel: 703-548-6284
Fax: 703-683-8396

Gary M. Nath
Registration No. 26,965
Gregory B. Kang
Registration No. 45,273
Teresa M. Arroyo
Registration No. 50,015
Customer No. 20529